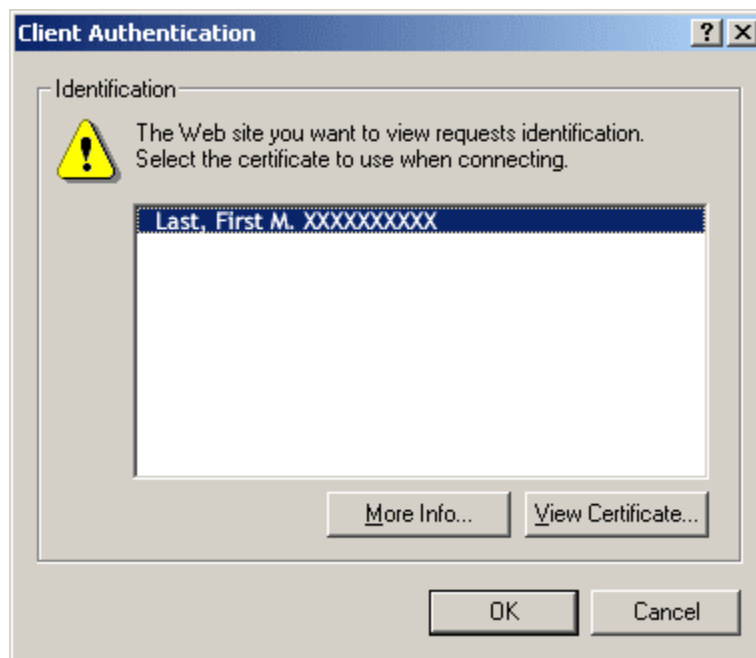


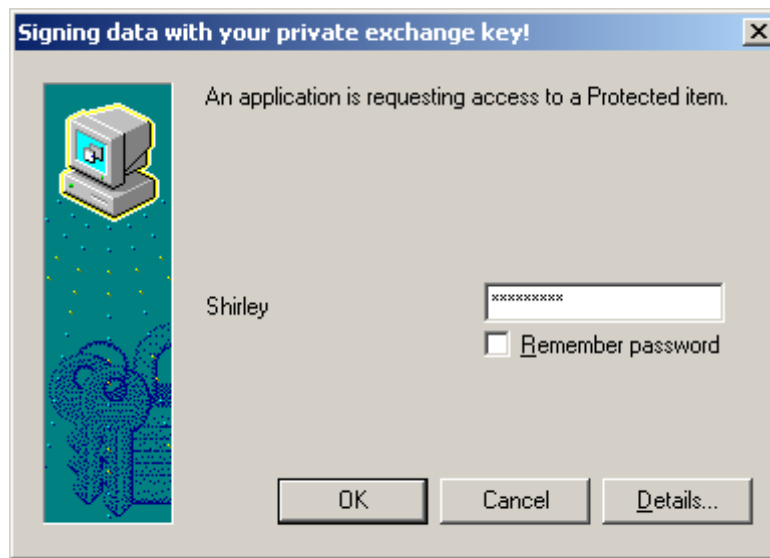
First Time User Setup Instructions for Accessing the DTS Self Support Help Desk

Access to the DTS Self Support Help Desk over Secure Socket Layer (SSL) requires a valid DoD issued Public Key Infrastructure (PKI) Certificate. If you are using a Common Access Card (CAC), go to the instructions for **Registering Your CAC Certificates with the ActivCard Middleware** before you proceed to step one. If you are using a Soft Token, go to the instructions for **Loading a Soft Token into the Microsoft Certificate Store** before you proceed to step one.

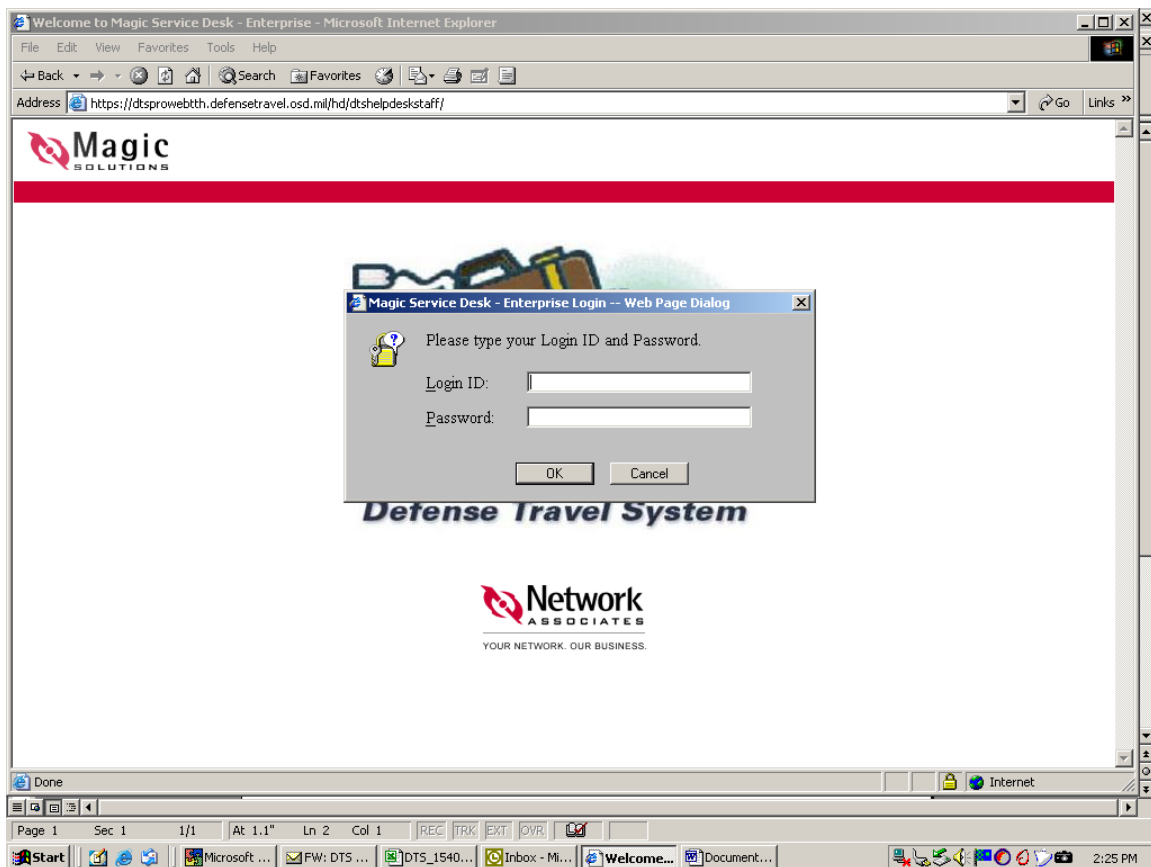
1. Click on the following link, <https://dtsprowebtth.defensetravel.osd.mil/hd/dtshelpdesk/>, to gain access to the DTS Self Support Help Desk. (Please make sure your PKI Certificate has been successfully imported into the browser before you proceed.)
2. When the Client Authentication window pops open, select the certificate you would like to use and click "OK".




3. When prompted, "An application is requesting access to a Protected item," enter your certificate password and Click "OK." Note: As a security precaution, you should never check the "Remember Password" box since that would allow access to your private key without entering a password.



4. From the DTS Self Support Login Screen, authorized callers can use their Magic Login ID and Password to gain access to the DTS Self Support Help Desk.



Note: If you are an Authorized caller and do not have a user login name or password, please click "Register now!"

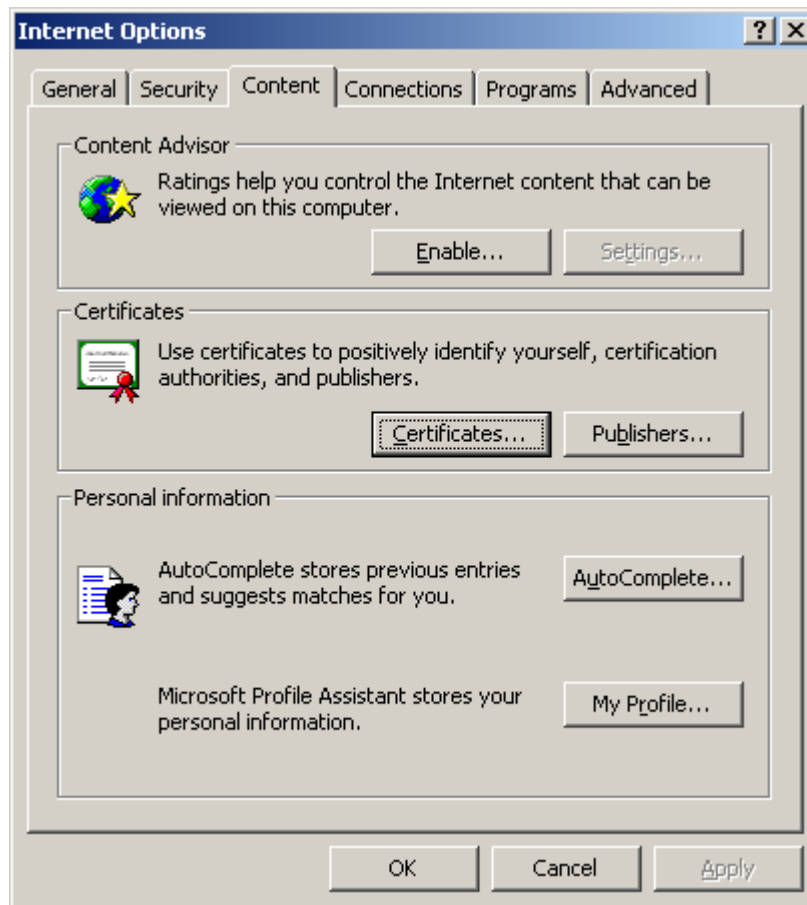
DTS Help Desk	
Sign Into DTS Tier 3 Help Desk	Register with Help Desk Self Support 
Client ID: <input type="text"/>	<ul style="list-style-type: none">• Registration for New Tier 3 Authorized Callers.• You will receive account confirmation within 2 business days of registration.
Password: <input type="password"/>	
Forgot your Password? Trouble Registering?	Register now!
<input type="button" value="Sign In"/>	
<small>Powered By Magic Solutions. Copyright c 1996-2001 Network Associates, Inc. and its affiliated Companies. All Rights Reserved.</small>	

Loading a Soft Token into the Microsoft Certificate Store

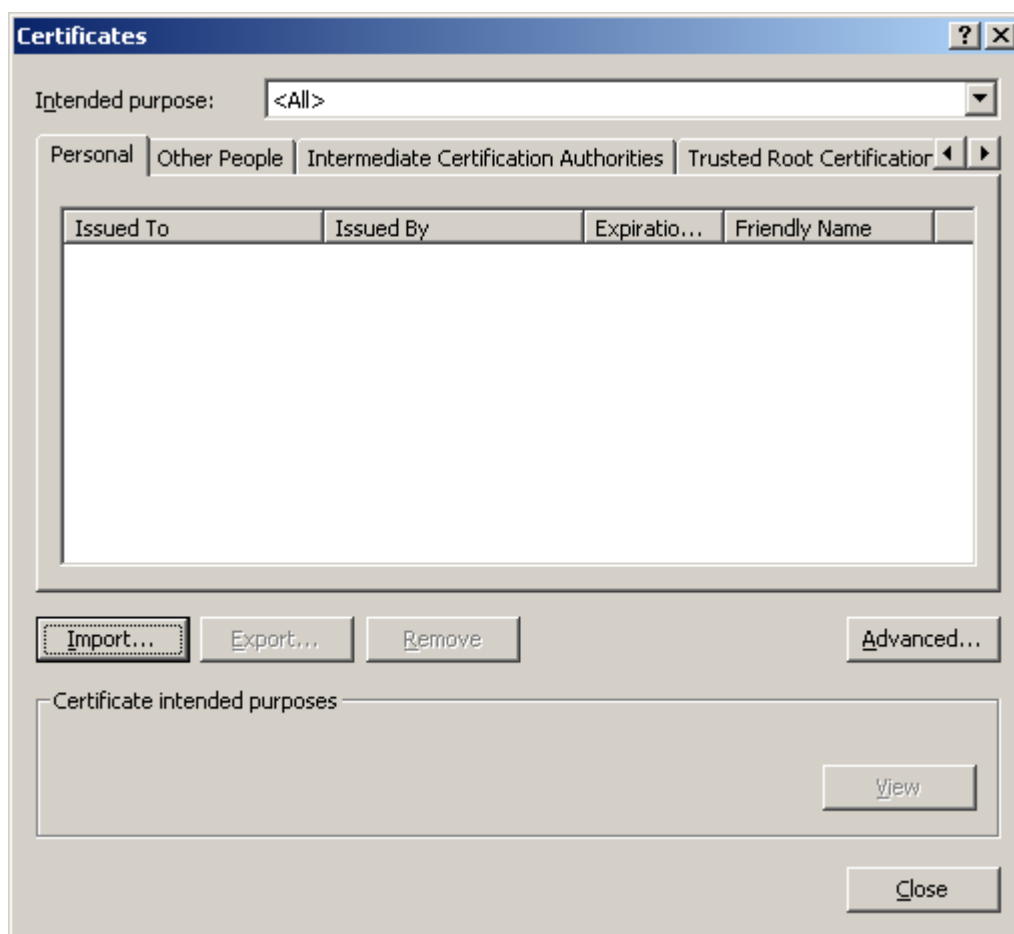
A PKI Certificate stored on a floppy disk (i.e., a “soft token”) must be imported into the user’s browser prior to accessing the DTS Self Support Help Desk.

Follow these steps to import the PKI Certificate into your browser.

1. Locate your valid DoD issued PKI Certificate.
2. Open Microsoft Internet Explorer.
3. From the “Tools” menu select “Internet Options”.
4. Go to the “Content” tab and click the “Certificates” button.



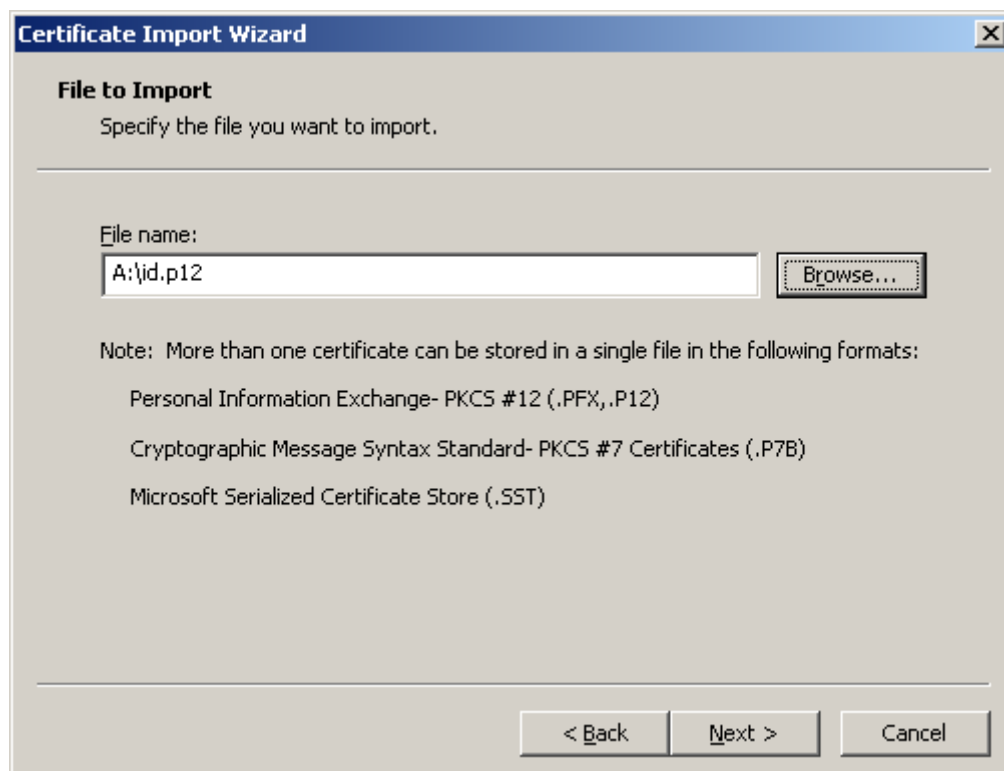
5. On the Certificates screen, choose the “Import” button.



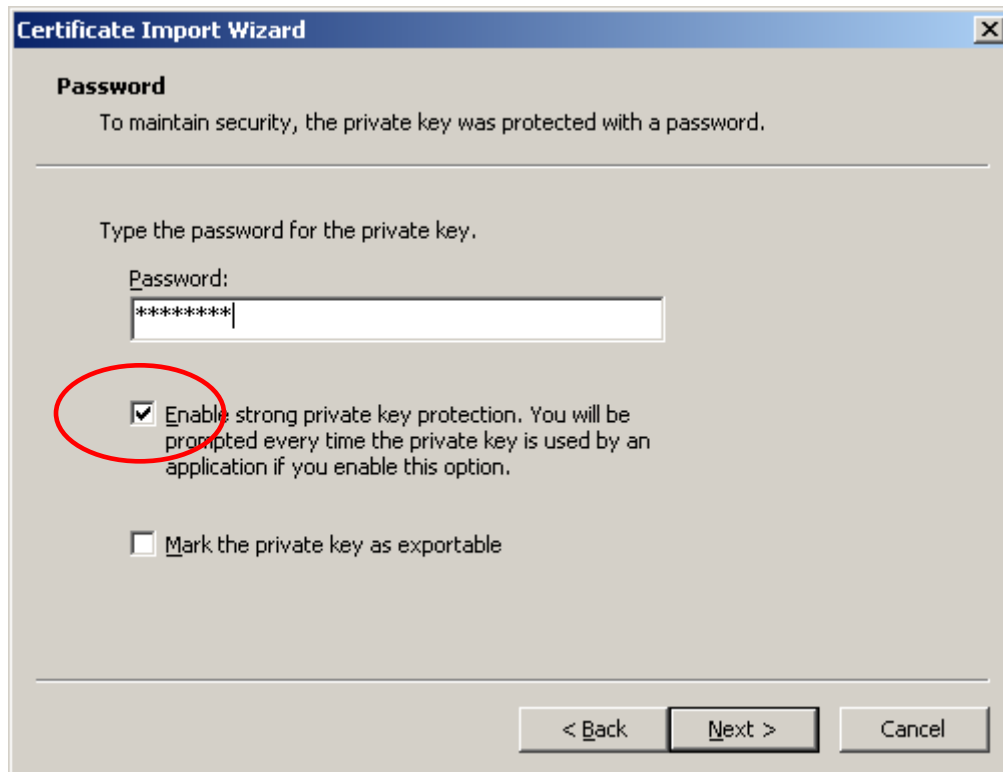
- When prompted on the Certificate Import Wizard, click "Next".



- Inside the "File name" dialog box, enter the location and name of your DoD issued PKI Certificate file from step one (you may also use the "Browse" button to locate the file) and click "Next".

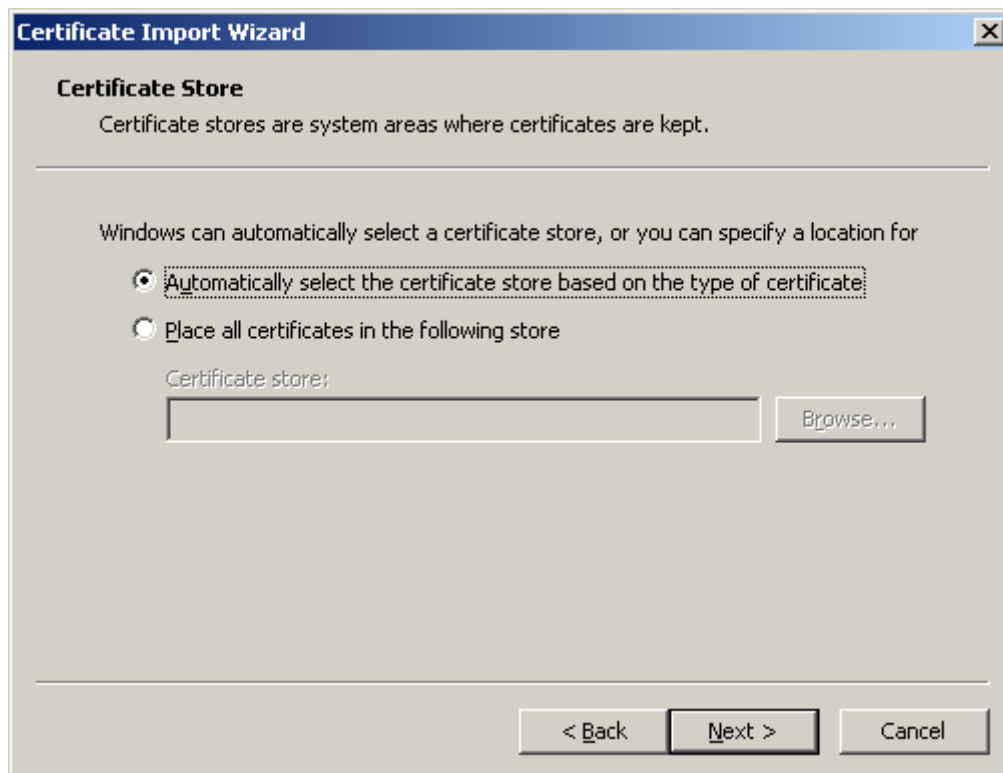


8. Enter the password for your certificate file, check the “Enable strong private key protection...” box, and click “Next”.



The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Password' step. The title bar reads 'Certificate Import Wizard'. Below the title bar, the section is titled 'Password'. A message states: 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a text box labeled 'Password:' containing several asterisks. Below the text box, there are two checkboxes. The first checkbox is checked and is circled in red; its label is 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' The second checkbox is unchecked and its label is 'Mark the private key as exportable'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. When prompted for a Certificate Store, click “Next”.



The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Certificate Store' step. The title bar reads 'Certificate Import Wizard'. Below the title bar, the section is titled 'Certificate Store'. A message states: 'Certificate stores are system areas where certificates are kept.' Below this, it says 'Windows can automatically select a certificate store, or you can specify a location for'. There are two radio buttons. The first radio button is selected and its label is 'Automatically select the certificate store based on the type of certificate'. The second radio button is unselected and its label is 'Place all certificates in the following store'. Below the second radio button, there is a text box labeled 'Certificate store:' and a 'Browse...' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

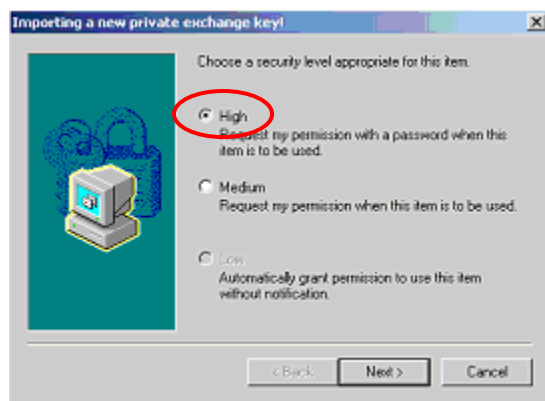
10. After reviewing the settings, click “Finish”.



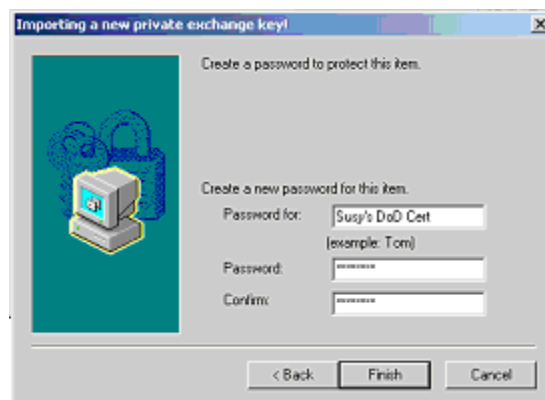
11. When prompted in the “Importing a new private exchange key!” window, click “Set Security Level”.



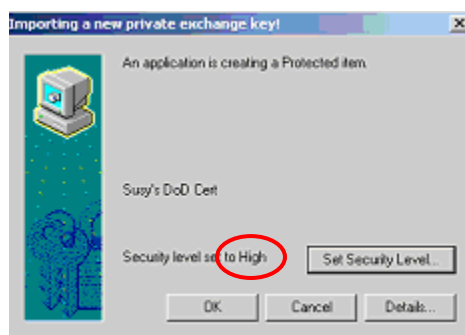
12. When prompted in the “Importing a new private exchange key!” window, select “High”. This will cause you to be prompted for a password whenever access to your certificate is required by an application. Click “Next”.



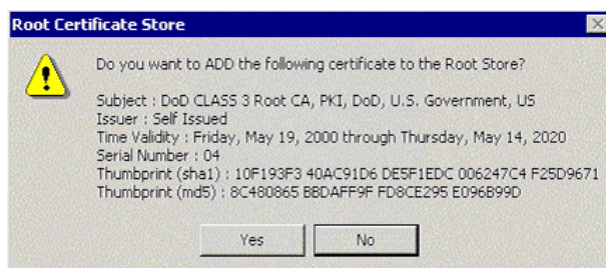
13. Enter a short descriptive name for the certificate and then enter the password you want to use to control access to the certificate. Re-enter the password to confirm. Click “Finish”.



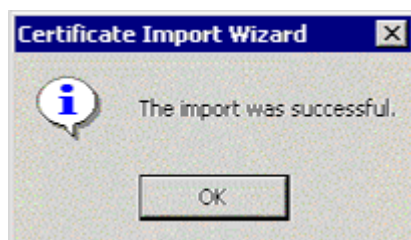
14. The security level has been changed to **HIGH**. Click “OK.”



15. When the Root Certificate Store prompts, "Do you want to ADD the following certificate to the Root Store?" click "Yes". Note: You may not receive this prompt if you have previously imported any DoD PKI Certificates into your browser.



16. The Certificate Import Wizard window should notify you that the import was successful. Click "OK".



17. Click "Close" in the Certificates window and click "OK" in the Internet Options window.

Upon successful registration of your PKI Certificate using a Soft Token, you may proceed to step one of the **First Time User Setup Instructions for Accessing the DTS Self Support Help Desk**.

Registering Your CAC Certificates using the ActivCard Middleware

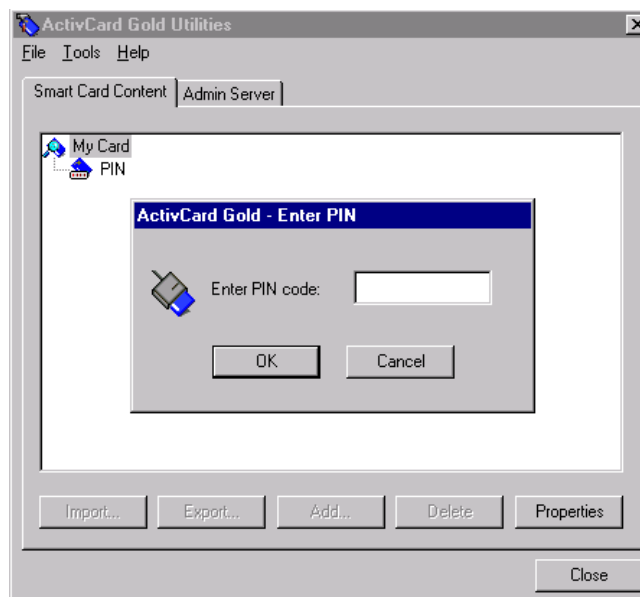
These instructions are for registering PKI Certificates stored on your Common Access Card (CAC) with the Microsoft Certificate Store using the ActivCard Gold Middleware for CAC. If you are using middleware other than ActivCard, please follow that manufacturer's recommendations for registering your CAC Certificates.

To register your certificate using ActivCard Gold Middleware, perform the following steps:

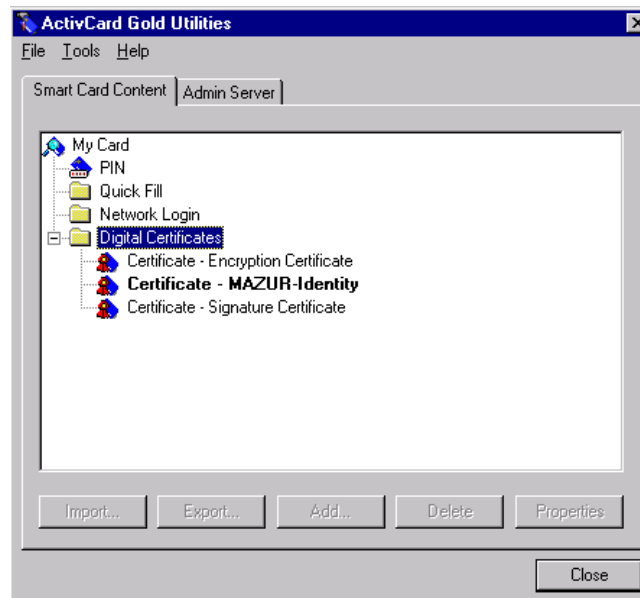
1. Insert your CAC into the reader.
2. Double click on the ActivCard icon in the System Tray to start the ActivCard Gold Utilities.



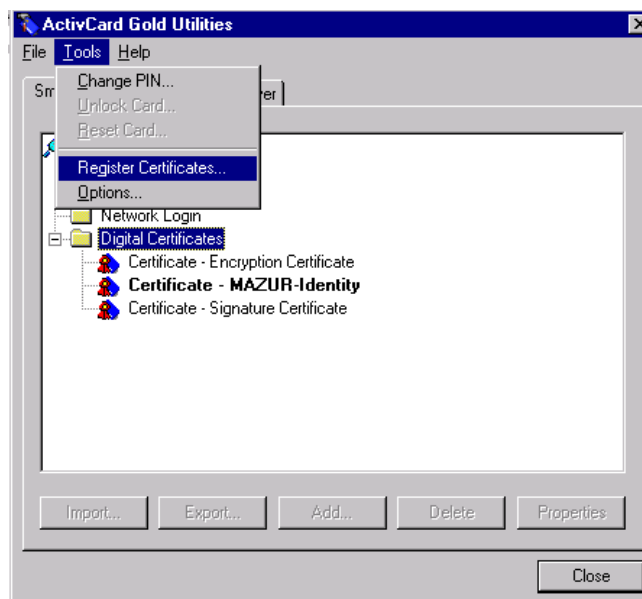
3. When prompted enter the CAC PIN.



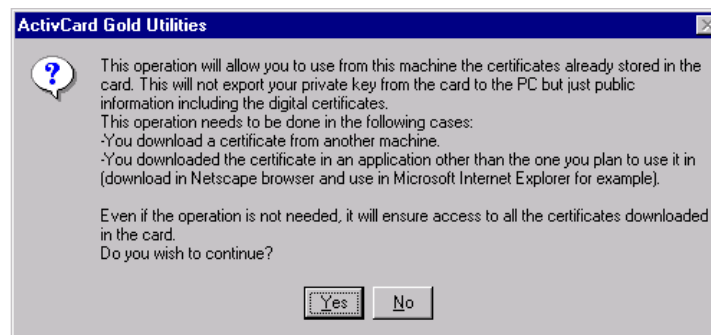
4. Wait until the card activates.



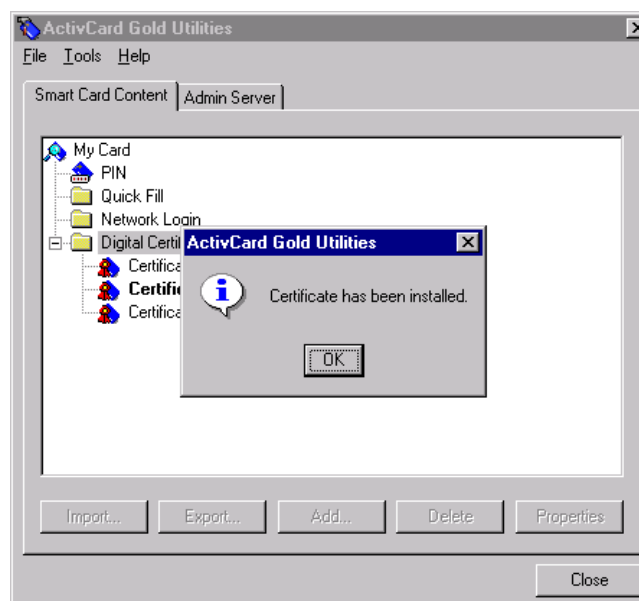
5. From the "ActivCard Gold Utilities" window, select the "Tools" option, then select "Register Certificates".



6. When prompted, Click “Yes”.



7. The “ActivCard Gold Utilities” window should notify you that the registration was successful. Click “OK”.



8. Click “Close” in the “ActivCard Gold Utilities” window.

Upon successful registration of your PKI Certificates using your CAC, you may proceed to step one of the **First Time User Setup Instructions for Accessing the DTS Self Support Help Desk**.

The above instructions are specific to ActivCard Gold Middleware. Since each middleware operates slightly differently, refer to your middleware documentation or online help if you are experiencing problems with a different middleware product.